

PATENT

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Inventor: Medvinsky, et al.) Confirmation No.: 7559
) Customer No.: 000043471
U.S. Serial No.: 09/890,180) Art Unit: 2135
Filed: January 28, 2000) Examiner: To, Bao Tran N.
)

Title: KEY MANAGEMENT FOR TELEPHONE CALLS TO PROTECT
SIGNALING AND CALL PACKETS BETWEEN CTA'S

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REMARKS FOR PRE-APPEAL BRIEF REQUEST FOR INTERVIEW

Dear Sir:

Applicants respectfully submit that the Examiner's rejections include clear errors because one or more limitations are not met by the cited reference.

I. Rejection under 35 U.S.C. § 102(b)

Claims 1-4, 6-9, and 11-19 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Barkan (European Patent Application No. EP 0738085). Applicants disagree.

Barkan discloses an "Apparatus for transferring the encryption key in a secure way, to facilitate establishing a secure communication link, comprises a key management device attaching to each user's encryption machine for the purpose of key distribution, and a secure encryption key distribution center. A key management device is attached to each user's encryption machine, containing a list of secure communication partners and their respective encryption keys. The encryption key and other parameters are transferred automatically to the encryption machine. The called machine receives the caller

identification, and the encryption key and other parameters are transferred automatically. The device displays to each user the true, reliable identity of the other party. If the desired addressee data is not found in the local data list, the key management device connects a secure key distribution center. The communication with the key distribution center is protected by encryption using the public key method. The key distribution center creates, for each user, a "certificate" which includes the user public key, user identification and issue date, all encrypted with the center's private key. The certificate can be used to access a multitude of remote databases or other information services on an irregular basis, without the need to subscribe to all of them. It may be also used for secure payment over insecure links using credit cards and/or for caller identification. The certificate method is used for flexible authorization schemes, to indicate changing time period of validity or authorizations/ permits."

Applicants submit that Barkan fails to disclose "generating a secret key at the gateway controller", "distributing the generated key to both telephony adapters", or "telephony adapters", as recited by Applicants' independent claims 1, 6, 11, and 15.

The present invention, in one embodiment, "provides a gateway controller that creates a media stream encryption key that is used to encrypt and decrypt messages between users. When a first user attempts to establish a secure channel with a second user, the gateway controller (source) associated with the first user, creates the media stream encryption key, sends the key inside a signaling message to the gateway controller (destination) that services the second user. The two gateway controllers then send the key to the two CTAs, that service the first and second user. This allows the two CTAs,

and thus, the two users to quickly establish a secure communication channel in the IP telephony network.” (See Applicants’ Specification, page 2, lines 16-24)

For a valid anticipation rejection, the Office must show that each limitation from the claims appears in a single piece of prior art. Applicants believe significant limitations from the independent claims are not taught in the Barkan reference. More specifically, Barkan does not teach (1) the step of generating a secret key at the gateway controller, (2) the step of distributing the generated key to both telephony adapters, or (3) the telephony adapters of the claims. Each of the independent claims generally teach these elements, and thus, the elements will be addressed for the claims as a group.

(1) *generating a secret key at the gateway controller:* The claimed embodiments recite generating a secret key at a gateway controller. However, the Barkan reference teaches something quite different. The Office Action indicates that the “key distribution center” of Barkan reads on the gateway controller of the claims. (See Office Action, page 3, line 4; page 4, line 15; page 6, line 5; page 8, line 10) However, it is not the key distribution center that is generating the key at issue in Barkan. Instead, it is the addressee (i.e., facility 3, the second user) in Barkan who generates the key at issue. (See Barkan, col. 6, lines 24-29; col. 16, lines 17-21) Barkan describes a procedure where the addressee generates a public key to be transmitted to the key distribution center, which forwards the key to the initiator. It is not taught, disclosed, or suggested that the key distribution center generate this particular key.

(2) *distributing the generated key to both telephony adapters:* The claims further call for the gateway controller to distribute the secret key to the first and second telephony adapters. The Office Action asserts that Barkan reads on this limitation,

indicating that the initiator and addressee read on the telephony adapters of the present claims. However, the Office Action cites portions of Barkan which describe a key distribution center which forwards the public key from the addressee to the initiator. (Office Action, page 3, lines 9-11; page 5, lines 9-10; page 6, lines 16-19; page 8, lines 12-17; citing Barkan, col. 3, lines 17-25; col. 6, lines 35-40; col. 7, lines 45-50) Thus, in Barkan, the public key is forwarded to an initiator, but is distributed *from*, instead of *to*, the addressee. Therefore, Barkan clearly fails to teach what is recited in Applicants' claims. Namely, that the secret key is distributed from the gateway controller to both the first and second telephony adapters.

(3) *telephony adapters:* The telephony adapters of the claims are directed at "achieving secure communication in an IP telephony network". (Applicants' Specification, page 3, lines 23-26) The Office Action states that facility 1 and 3 in Barkan read on the telephony adapters of the claims. (Office Action, page 3, lines 4-6) However, there is no teaching, disclosure, or suggestion in Barkan that these "facilities" each be used as an IP telephony adapter.

In view of the above arguments, Applicants submit that independent claims 1, 6, 11, and 15 are patentable over Barkan. Claims 2-4, 7-9, and 12-14, and 16-19 are patentable at least by virtue of depending from their respective base claim. Applicants respectfully request withdrawal of the rejection.

II. Rejection under 35 U.S.C. § 103(a)

Claims 5 and 10 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Barkan in view of Ganesan (U.S. Patent No. 5,535,276, issued July 9, 1996) (Ganesan). Applicant respectfully disagrees.

As stated above in Section I., Barkan fails to disclose “generating a secret key at the gateway controller”, “distributing the generated key to both telephony adapters”, or “telephony adapters”. The Examiner conceded that Barkan fails to disclose “receiving a request at the first gateway controller to provide the secret key to a law enforcement server; and providing the secret key to the law enforcement server”. In order to cure the Examiner’s perceived deficiency of Barkan, Ganesan is cited.

Ganeson discloses a system and method for securing communications using split private key asymmetric cryptography. However, Ganeson, like Barkan, also fails to teach, disclose, or suggest “generating a secret key at the gateway controller”, “distributing the generated key to both telephony adapters”, or “telephony adapters”, as recited in claims 1, 6, 11, and 15. As such, the combination of Barkan and Ganeson fail to teach what is recited by Applicants’ claims.

In view of the above arguments, Applicants submit that claims 5 and 10 are patentable over Barkan in view of Ganeson. Applicants respectfully request withdrawal of the rejection.

Date: August 8, 2006

Respectfully submitted,

By: /Thomas Bethea, Jr./

Thomas Bethea, Jr.

Reg. No.: 53,987

Motorola Connected Home Solutions
101 Tournament Drive
Horsham, PA 19044
(215) 323-1850

PRE-APPEAL BRIEF REQUEST FOR REVIEW		Docket Number (Optional) D02236-02
	Application Number 09/890180	Filed 01/28/2000
	First Named Inventor Medvinsky	
	Art Unit 2135	Examiner To, Bao Tran N.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).

Note: No more than five (5) pages may be provided.

I am the

<input type="checkbox"/>	applicant inventor.	/Thomas Bethea, Jr./ Signature
<input type="checkbox"/>	assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)	Thomas Bethea, Jr. Typed or printed name
<input type="checkbox"/>	attorney or agent of record. Registration number _____	215-323-1850 Telephone number
<input checked="" type="checkbox"/>	attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34: <u>53,987</u>	August 8, 2006 Date

NOTE: Signatures of all the inventors or assignees or record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*

*Total of 1 forms are submitted.